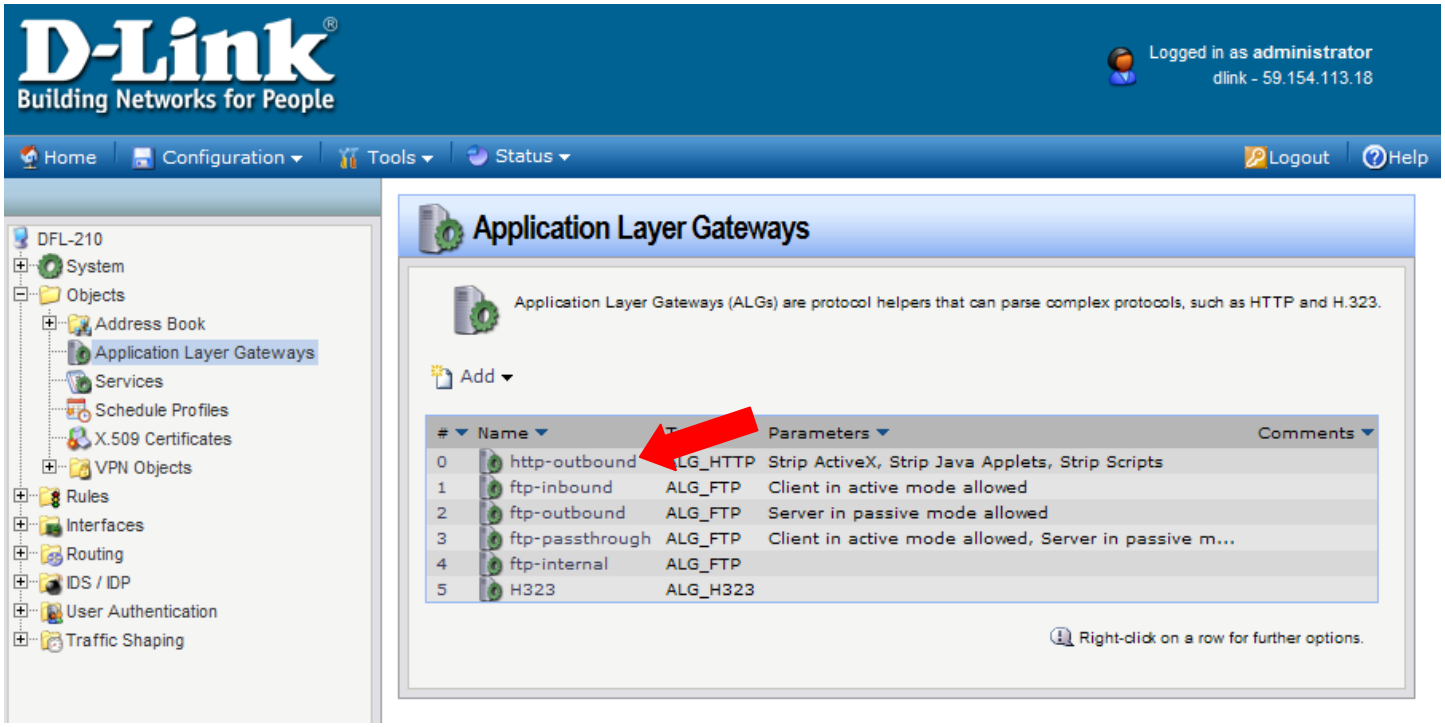
How to setup Web filters
in DFL-210/800/1600/2500 VPN Firewall

You can set your firewall to block access to certain Web sites. This setup example shows two ways of setting the filters up:

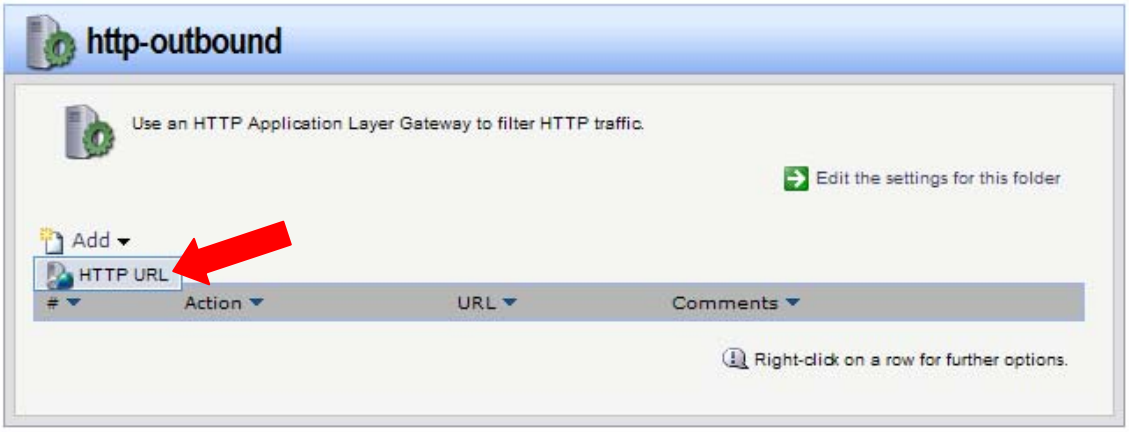
A. Blocking specific sites and allowing access to all other Web sites.
B. Allowing access to specific sites and blocking all other HTTP access;

Step 1. Log into the Firewall by opening Internet Explorer and typing the LAN address of the Firewall. In our example we are using 192.168.1.1. Enter Username and Password which you specified during the initial setup of the Firewall.

Step 2. Click on Objects > Application Layer Gateways. Click on “http-outbound”.



Click on “Add” and select “HTTP URL”

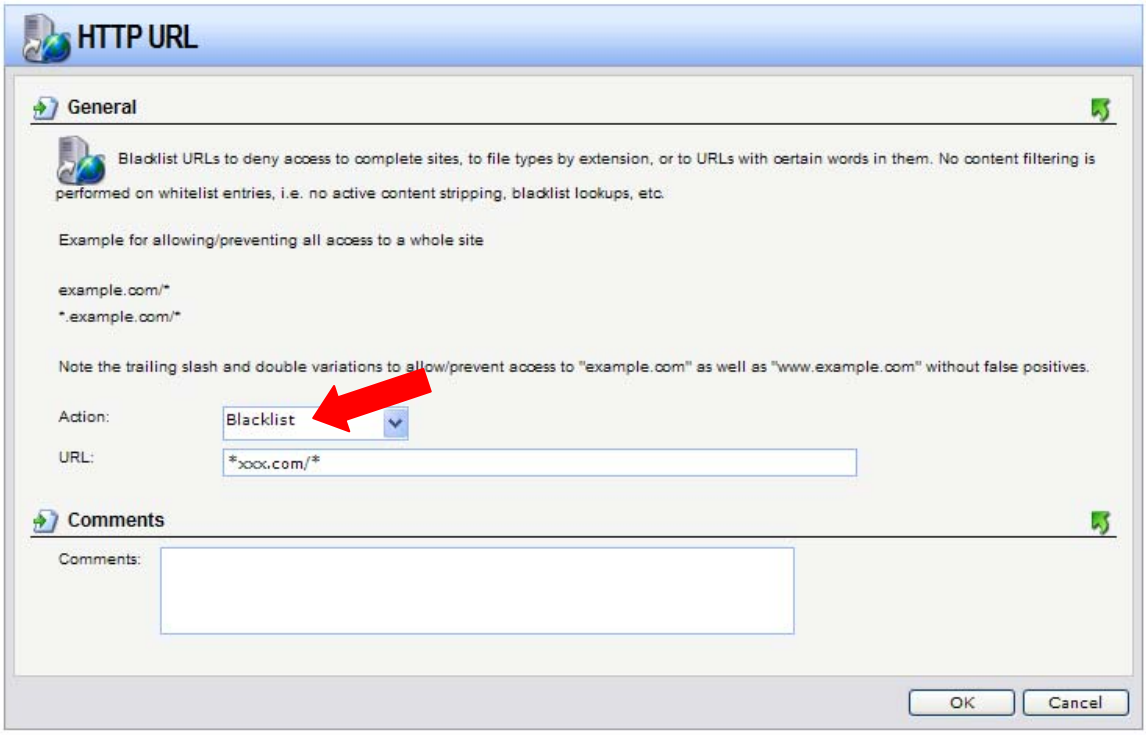


Step 3. Setting Blacklists and Whitelists.

There are two ways of setting Web filters:

A. Blocking specific sites and allowing access to all other Web sites (“Blacklisting”).
or
B. Allowing access to specific sites and blocking all other HTTP access (“Whitelisting”);

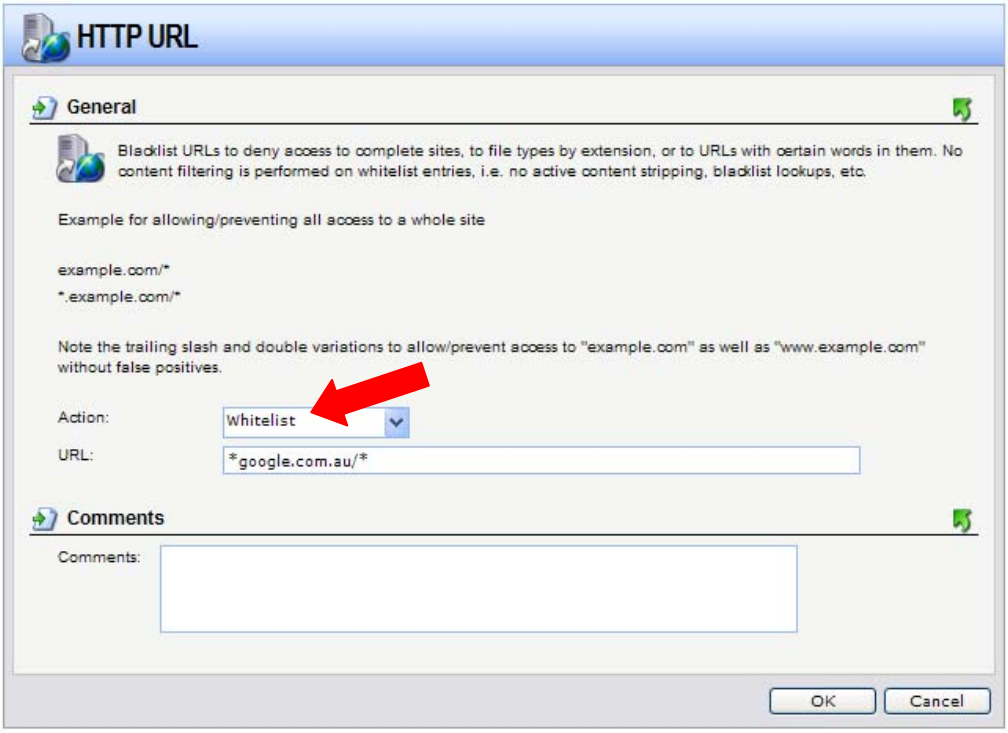
A. Blocking specific sites and allowing access to all other Web sites (Blacklisting).
When adding the HTTP URL object select “Blacklist” under Action. Enter in the Web site that you want to block. You can use wildcards (*), e.g. *xxx.com/*.
Click on OK.



To add more Web sites click on Add and select HTTP URL and repeat the above step.

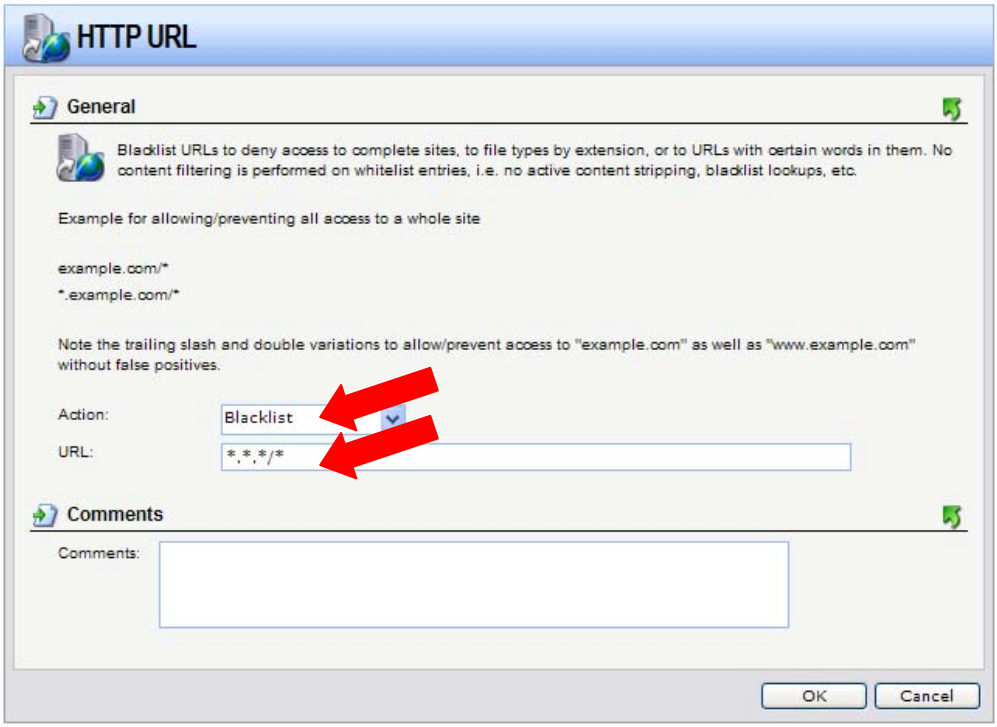
Note: You do not need to create an additional Whitelist because by default the firewall allows access to all websites.

B. Allowing access to specific sites and blocking all other HTTP access (Whitelisting).
When adding the HTTP URL object select “Whitelist” under Action. Enter in the Web site that you want to allow access to. You can use wildcards (*), e.g. *google.com.au/*.
Click on OK.



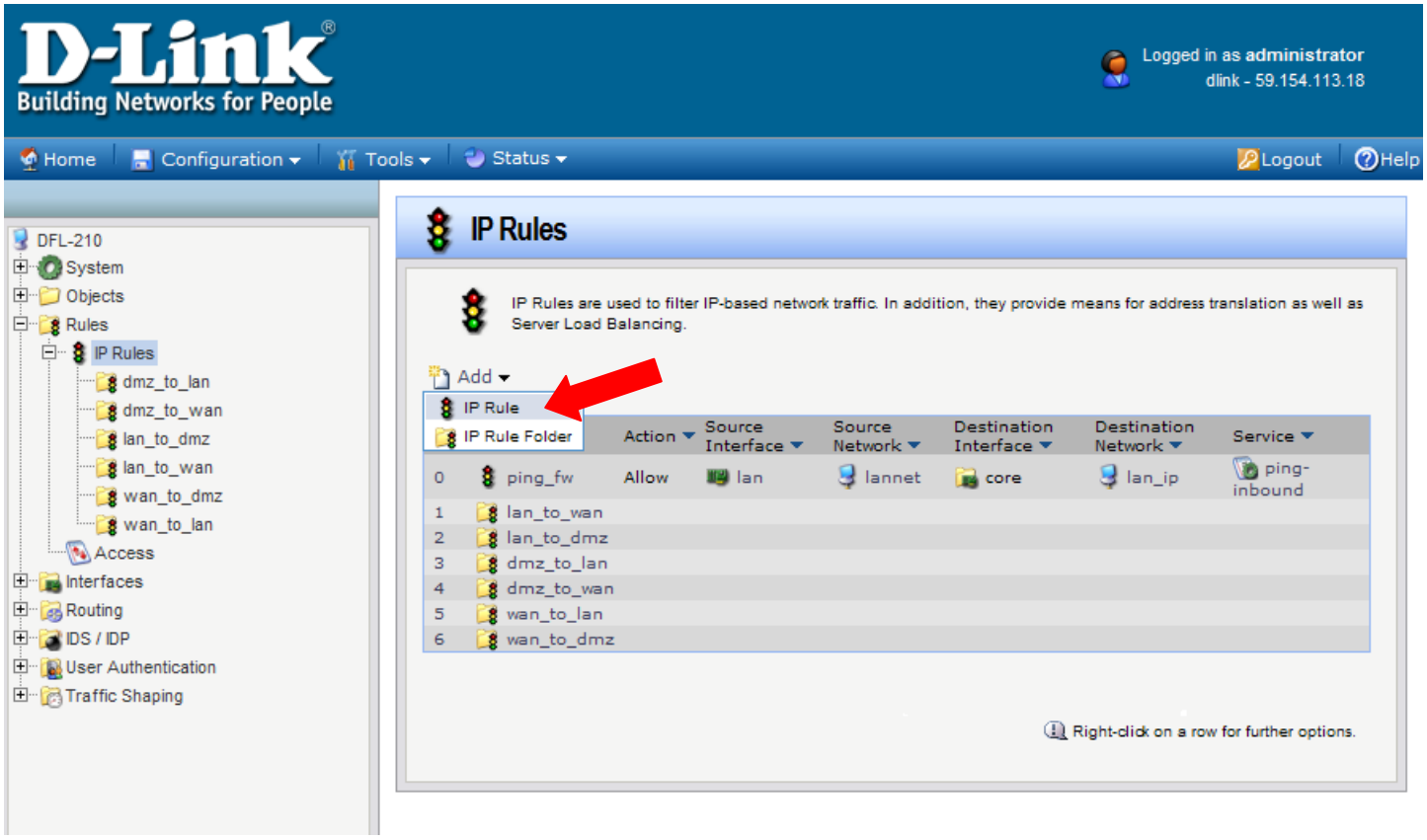
To add more Web sites click on Add and select HTTP URL and repeat the above step.

When using Whitelisting you need to add an additional HTTP URL entry which will block every other site.
Add another HTTP URL and select Blacklist under Action.
Under URL enter *.*.*/*.
Click on OK.



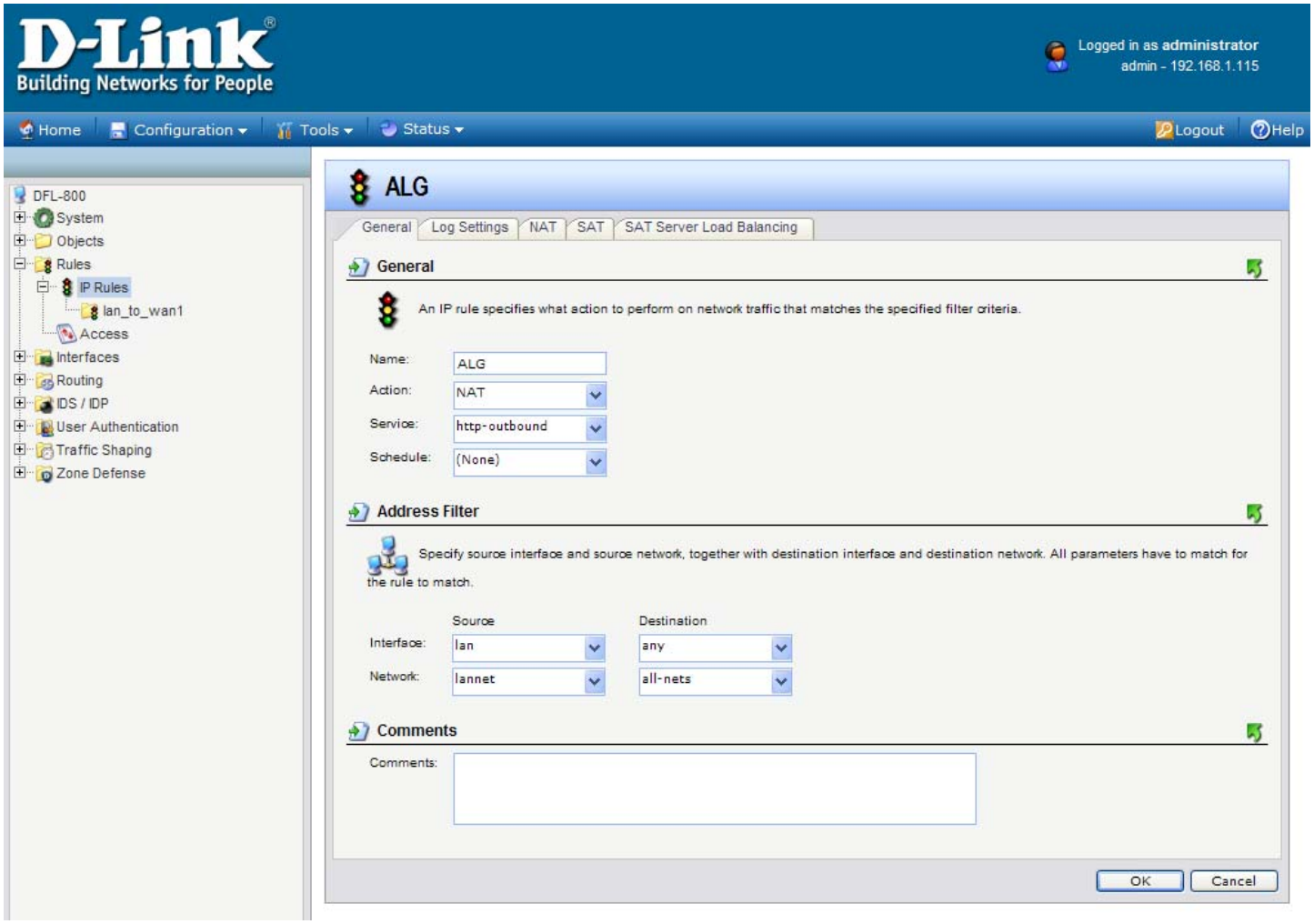
This Blacklist entry should be the last one on the list (the final Blacklist *.*.*/* entry is only required in Example B (Allowing access to specific sites and blocking all other HTTP access). Example A will only have a list of Blacklist entries for specific Web sites.

Step 4. Add an IP Rule.
Go into Rules > IP Rules.
Click on “Add” and select “IP Rule”.

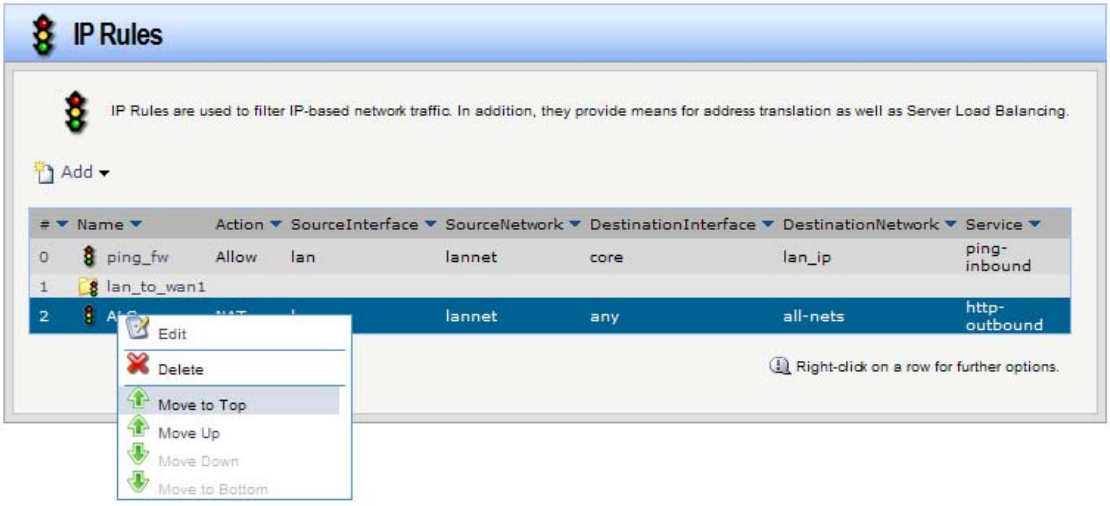


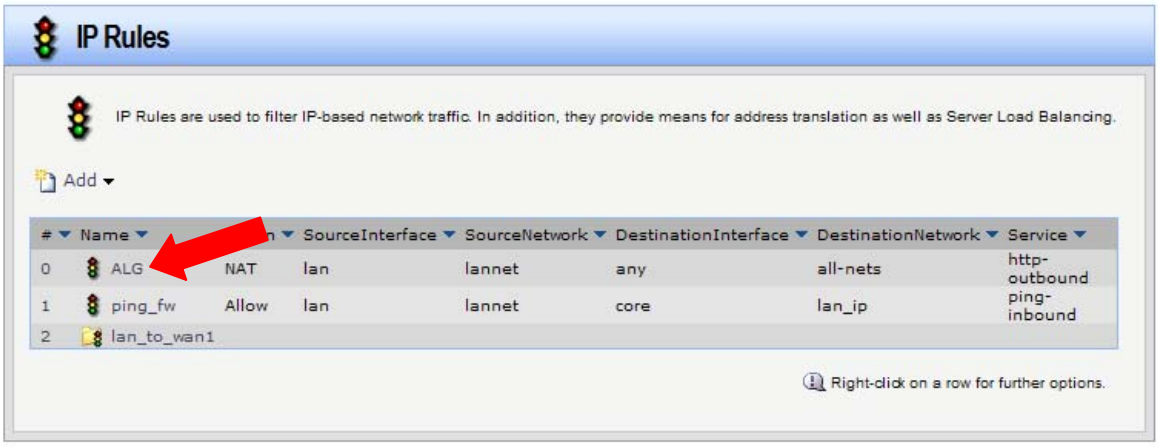
Specify the following settings for the new IP Rule:
Name: (in our example we used “ALG”)
Action: NAT
Service: http-outbound (the Application Layer Gateway we configured in the previous steps)
Source Interface: lan; Source Network: lannet
Destination Interface: any; Destination Network: all-nets

Click on OK.

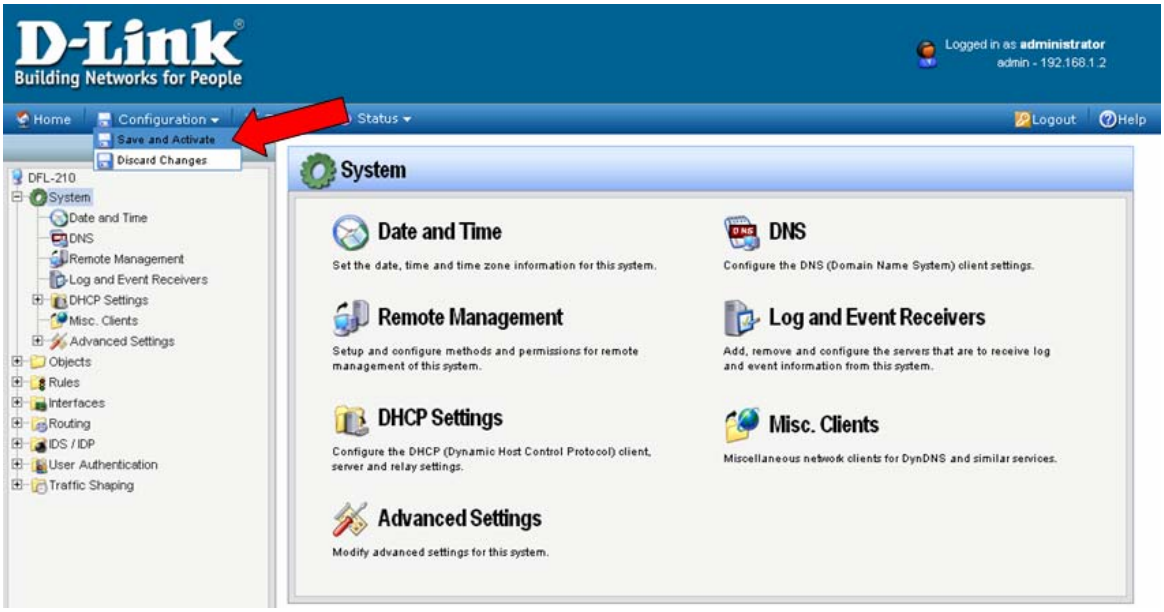


Step 5. Move the rule to the top of the list.
Right click on the new IP Rule “ALG” and select “Move to Top”.

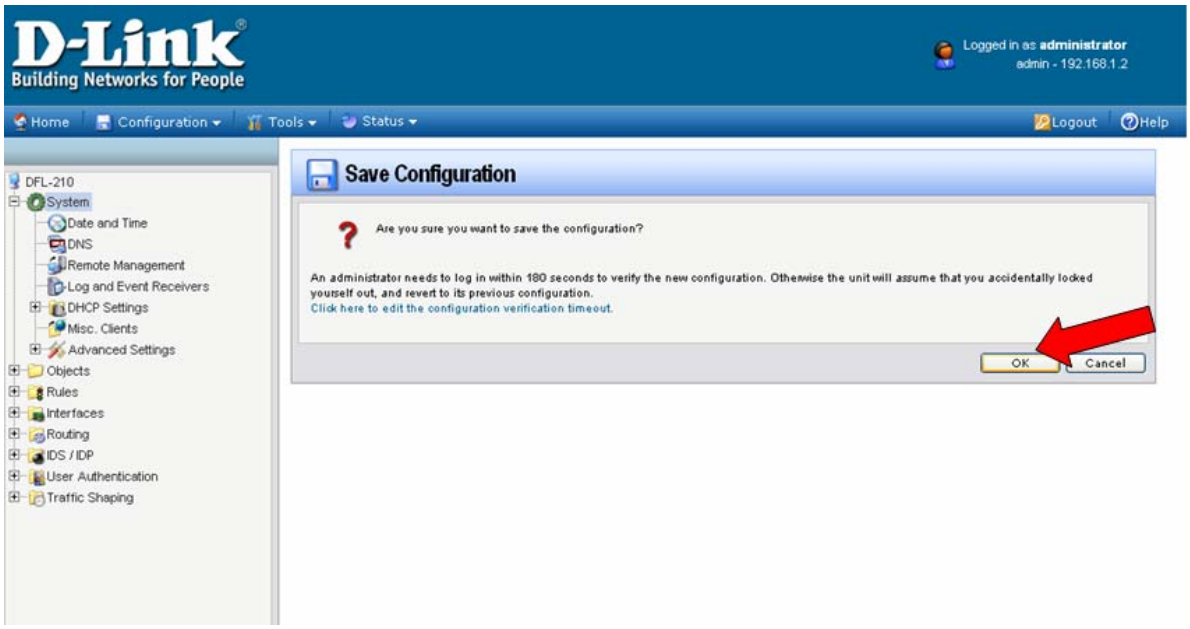




Step 6. Save the new configuration. In the top menu bar click on Configuration and select “Save and Activate”.



Click on OK to confirm the new settings activation:



Wait 15 seconds for the Firewall to apply the new settings.